UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/360,575	07/26/1999	SCOTT A. VANSTONE	2189-19	4374

616 7590 04/22/2004

THE MAXHAM FIRM
750 "B" STREET, SUITE 3100
SAN DIEGO, CA 92101

EXAMINER	
AKPATI, ODAICHE T	

ART UNIT	PAPER NUMBER
2135	11

DATE MAILED: 04/22/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/360,575	VANSTONE, SCOTT A.	
	Examiner	Art Unit	
	Tracey Akpati	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 8-18 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 8-18 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on 7/26/99 is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☒ Certified copies of the priority documents have been received in Application No. 08/790,545.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☒ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1, 3-8 were cancelled (claim 2 was not originally presented) and claims 9-19 were added in the amendment filed 2/6/04. Claims 9-19 are renumbered as 8-18 according to 37CFR1.126.

Priority

2. Acknowledgment is made of applicant's claim for foreign priority under 35 U.S.C. 119(a)-(d). The certified copy has been filed in parent Application No. 08790545, filed on 1/30/1997. The date applicable for foreign priority is 1/31/1996 instead of the erroneous date of 1/31/1995.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 8-13,17 and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ishiguro et al (5396558) in view of Gifford (6049785).

With respect to Claim 8, Ishiguro et al meets the limitation of "a method of performing a transaction between a first and a second participant wherein said second participant permits a service to be provided to said first participant in exchange for a payment" in the abstract and on column 1, lines 1-15; and "said first participant verifying the legitimacy of said second

participant to obtain assurance that said service will be provided upon payment" on column 2, lines 52-56; and "said second participant verifying the legitimacy of said first participant to obtain assurance that payment will be secured upon provision of said service" on column 2, lines 43-47. Ishiguro et al however discloses a master digital signature instead of a digital signature being verified by the IC card terminal (i.e. second participant). Gifford discloses a digital signature as shown below.

The limitation of "said second participant obtaining a digital signature for said first participant on said transaction whereby said second participant may obtain payment from a third participant" is met by claim 11 of Gifford.

In Ishiguro et al, the IC card represents the first participant, while the IC card terminal represents the second participant. In the last three sentences of the abstract, mutual verification/authentication occurs between the IC card and the terminal, before a service is provided.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Gifford within the system of Ishiguro et al because the master digital signature can be easily substituted with the digital signature, which is a common well known means of authentication. A digital signature protects the communication between the IC card and terminal from a replay attack (Gifford, column 4, lines 24-27), which is a common attack used to defraud unprotected businesses and customers.

With respect to Claim 9, the limitation of "wherein said first participant is a holder of a card which performs cryptographic operations" is met by Ishiguro et al on column 2, lines 16-25. The cryptographic operations are disclosed on column 2, lines 26-61.

With respect to Claim 10, the limitation of "wherein said second participant is a terminal" is met by Ishiguro et al on column 2, lines 43-47.

With respect to Claim 11, all the limitation is met by Ishiguro et al except the limitation of a financial institution being the third party. Ishiguro et al however reveals a third party as a management center that verifies the user at the terminal on column 1, lines 29-40.

The limitation of "wherein said third participant is a financial institution" is met by Gifford on column 3, lines 46-51.

It would have been obvious to one of ordinary skill in the art at the time the nvention was made to combine the teachings of Gifford within the system of Ishiguro et al because a financial institution as a third party in the verification of an IC card user is a commonly used method of ensuring that the user is who he claims to be and consequently hold him responsible for payment of services, in the event of a default of payment.

With respect to Claim 12, the limitation of "said second participant sending a first message to said first participant, the first message including details and credentials of said second participant" is met by Ishiguro et al on column 2, lines 48-51; and "said first participant

verifying said transaction details and said credentials" is met also by Ishiguro et al on column 2, lines 52-56.

With respect to Claim 13, Ishiguro et al meets the limitation of "said first participant sending a second message to said second participant, said second message including credentials of said first participant" on column 2, lines 40-42; and "said second participant verifying said credentials of said first participant" on column 2, lines 43-47.

With respect to Claim 17, the limitation of "wherein said credentials include a public key certificate" is met inherently by Ishiguro et al on column 2, lines 52-56. The presence of a public key and terminal identification number being used to verify validity of a digital signature requires the presence of a public key certificate.

With respect to Claim 18, all the limitation is met by Ishiguro et al except the limitation disclosed below.

The limitation of "wherein said challenge is a nonce" is met by Gifford on column 2, lines 63-64 and column 3, lines 41-45.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Gifford within the system of Ishiguro et al because a challenge being a nonce requires that the challenge be unique and hence hard to guess. Therefore an attacker would not be able to easily guess the challenge used to conclude the

transaction, so this could be used as a final hurdle to prevent a persistent attacker from being able to mimick or replay a real transaction.

Claims 14, 15, and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ishiguro et al (5396558) in view of Gifford (6049785) in further view of Chaum (5276736).

With respect to Claim 14, all the limitation is met by the combination of Ishiguro et al and Gifford except the limitation disclosed below.

Chaum meets the limitation of "said second participant generating a response to said challenge" on column 3, lines 57-60; and "said second participant sending a third message including said response to said first participant" on column 3, lines 57-60; and "said first participant verifying said response" on column 3, lines 52-55 and 57-62; and "said first participant sending a fourth message to said second participant such that said digital signature is provided by said second message and said fourth message" on column 4, lines 20-27, 57-60. The message being signed reflects a digital signature being appended to the message being sent.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Chaum within the combination of Ishiguro et al and Gifford because verification of the challenge prevents an outside attacker from using a replay attack to gain access to the system. The challenge is unique and once verified, provides a greater guarantee that the transaction is in fact legitimate.

With respect to Claim 15, all the limitation is met by the combination of Ishiguro et al and Gifford except the limitation disclosed below.

Chaum meets the limitation of "said second participant verifying information in said fourth message" on column 4, lines 20-27; and "said second participant completing said transaction by providing said service" inherently on column 4, lines 44-47 and 57-60; and "said second participant sending said third participant a subset of said first, second, third and fourth messages to obtain payment" on column 4, lines 35-45.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Chaum within the combination of Ishiguro et al and Gifford because since the third party/financial institution does not aggressively authenticate the user, it will then need a copy of the verification information/output to be able to determine if payment should be authorized on behalf of the user to the second participant.

With respect to Claim 16, all the limitation is met by the combination of Ishiguro et al and Gifford except the limitation disclosed below.

The limitation of "said third participant verifying said subset" is met by Chaum on column 4, lines 37-43; and "said third participant providing payment to said second participant" is met on column 4, lines 44-47.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Chaum within the combination of Ishiguro et al and Gifford because since the third party/financial institution does not aggressively authenticate the user, it will then need a copy of the verification information/output to be able to determine if payment should be authorized on behalf of the user to the second participant.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tracey Akpati whose telephone number is 703-305-7820. The examiner can normally be reached on 8.30am-6.00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 703-305-4393. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

OTA